UNITED STATES BANKRUPTCY COURT

CENTRAL DISTRICT OF CALIFORNIA – SANTA ANNA DIVISION

In re	:	Case No. 8:23-bk-10571-SC
THE LITIGATION PRACTICE GROUP, P.C.,	:	Chapter 11
Debtor.	:	

CONSUMER PRIVACY OMBUDSMAN

REPORT TO THE COURT

July 21, 2023

Lucy L. Thomson
Consumer Privacy Ombudsman

The Willard; Suite 400
1455 Pennsylvania Avenue, N.W.
Washington, D.C. 20004
lucythomson_cpo@earthlink.net
Telephone: (703) 212-8770

I. Privacy Ombudsman Report to the Court

A. Overview of the Privacy Issues

Pursuant to Bankruptcy Code section 332(b), Lucy L. Thomson, the Consumer Privacy Ombudsman ("CPO" or "Ombudsman") appointed in this case,[1] submits this Report to advise the Court on the issues related to the protection of the privacy of consumers of The Litigation Practice Group PC ("Debtor" or "LPG").

The Bankruptcy Code provides a framework in sections 332 and 363 for evaluating the sale or transfer of personal consumer records in the context of a bankruptcy case. 11 U.S.C. §§ 101 *et. seq*. The statute provides a broad mandate for the Ombudsman – to investigate and provide the Court with information relating to:

- The Debtors' Privacy Policy;
- Potential losses or gains of privacy to consumers if the sale is approved;
- Potential costs or benefits to consumers if the sale is approved; and
- Possible alternatives that would mitigate potential privacy losses or costs to consumers.

11 U.S.C. § 332.

In enacting sections 332 and 363, Congress has evidenced its intention to protect the privacy interests of consumers in connection with the bankruptcy sale of personal data. The Bankruptcy Code provides that in making that determination, the Court may: (1) consider whether the sale is consistent with the privacy policy; (2) give due consideration to the facts, circumstances,

[1] Order Directing the Appointment of a Consumer Privacy Ombudsman and Requiring Notice [ECF No. 226, filed 7/12/23]; United States Trustee Notice of Appointment of Consumer Privacy Ombudsman [ECF No. 251, filed 7/17/23], Order Approving the Appointment of a Consumer Privacy Ombudsman, October 27, 2022 [ECF No. 253, filed 7/17/23]. The Ombudsman has served as the CPO in 33 prior bankruptcy cases where privacy issues related to the sale of personal data were addressed.

and conditions of such sale; and (3) find that no showing was made that such sale would violate applicable non-bankruptcy laws.[2] 11 U.S.C. § 363(b)(1).

This Consumer Privacy Ombudsman (CPO) Report to the Court ("CPO Report") highlights key privacy issues for the Court's consideration and discusses them in the sections that follow. Because of the very short timeframe of only a few days available for the Ombudsman to assess the issues in this case, this CPO Report focuses on illegal LPG operations and failure to comply with applicable non-bankruptcy laws, due diligence and evaluating potential Purchaser(s) using the 'Qualified Buyer' criteria, and requirements/best practices for an Opt-In/Opt-Out process if the sale goes forward.

Illegal LPG Operations. A bankruptcy sale of personal consumer data must not violate applicable non-bankruptcy laws. The LPG clients were required to make upfront and periodic payments to the Debtor immediately upon signing a contract for services; often the payments were initiated and continued even though the consumers received no resolution of their debts. Federal and state laws make it illegal for companies to charge upfront fees from a client before they have settled or otherwise resolved a consumer's debts. LPG required payment using withdrawals from consumers' bank accounts. While the Telemarketing Sales Rule (TSR) gives clients the right to

[2] The CPO Process – Section 363(b)(1) of the Bankruptcy Code provides that the Court must make a number of determinations before the Debtors are authorized to sell the LPG personally identifiable consumer records. More specifically:

- If the Debtors' Privacy Policy prohibits the transfer of personally identifiable information about individuals to persons that are not affiliated with the Debtors; and
- If the policy is in effect on the date of the commencement of the case;
- Then the Trustee may not sell personally identifiable information to any person unless–

  (A) such sale is consistent with such policy; or

  (B) after appointment of a consumer privacy ombudsman in accordance with section 332, and after notice and a hearing, the court approves such sale or such lease –

  (i) giving due consideration to the facts, circumstances, and conditions of such sale; and

  (ii) finding that no showing was made that such sale would violate applicable non-bankruptcy law.

stop authorization of ACH payments at any time, LPG failed to respond to numerous requests, thus obtaining funds to which they were not entitled. These are only two examples of the many failures of LPG to abide by federal and state laws. The Bankruptcy Code would not permit the sale of a business such as LPG in violation of these applicable non-bankruptcy laws.

Due Diligence and the 'Qualified Buyer' Criteria. In evaluating the sale of client records, bankruptcy courts have utilized a due diligence framework in which they assessed whether the proposed Purchaser is a "Qualified Buyer," using criteria created in 2008 and first applied in the *Toysmart* case.[3] These criteria have been updated and followed in many subsequent bankruptcy cases for more than a decade.[4] Among the issues to be addressed are serious concerns[5] about the suitability of the proposed purchaser, Consumer Law Group, to provide services the LPG clients need and in a cost effective manner.

***Notice and Opt-in to a Sale of Personal Consumer Records*.** The Debtor LPG collected personal and financial data from tens of thousands of individuals (at least 40,000) who contracted to receive its debt relief and credit repair services.

[3] The State Attorneys General objected to the sale, arguing that because sensitive records about children and credit card numbers were being sold, consumers should be permitted to consent to the sale through an Opt-In procedure. Because the records were not sold within a specified period of time, they were destroyed. Objection of the Commonwealth of Massachusetts and 46 States to the Debtor's Motion to Approve Settlement with Federal Trade Commission and for Authority to Enter in Consent Agreement, page 8. *In re* Toysmart.com LLC, No. 00-13995-CJK (U.S. Bankr. Court, D. Mass.), ["*In re* Toysmart.com"] *available at* https://www.ftc.gov/legal-library/browse/cases-proceedings/x000075-toysmartcom-llc-toysmartcom-inc.

[4] *In re* Borders Group, Inc., No. 11-10614-mg (Bankr. S.D.N.Y.) (Glenn, J.), *In re* RadioShack Corporation, No. 15-10197 (BLS) (Bankr. D. Del.) (Shannon, J.); *In re* Choxi, 16-13131 (SCC) (Bankr. S.D.N.Y.) (Chapman, J.); *In re* Century 21 Department Stores, 20-12097 (Bankr. S.D.N.Y.) (Chapman, J.); *In re* KB US Holding 20-22962 (SHL) (Bankr. S.D.N.Y.) (Lane, J); *In re* MKJC Hyundai, 20-42283, (Bankr. S.D.N.Y.) (Mazer-Marino, J.); *In re* Loot Crate, 19-11791-BLS (Bankr. D. DE) (Shannon, J.); *In re* NovaSom, 19-11734 (BLS) (Bankr. D. DE) (Shannon, J.); *In re* Hobbico, 18-10055 (KG) (Bankr. D. DE) (Gross J.); *In re* Circuit City Stores, 3:08-bk-35653 (Bankr. E.D. VA) (Huennekens, J.); *In re* Linens N Things, 08-10832 (CSS) (Bankr. D. DE) (Sontchi, J.).

[5] Objections of Carolyn Beech and Diane Skarnavack to Motion for Sale of Property of the Estate Under Section 363(b) [Doc. No. 185, filed 7/7/23]

LPG published a privacy policy on its website to ensure the confidentiality of personal and financial consumer records. With a strict privacy policy in which LPG represented that "You have the right to opt out of the sale of your personal information," if the sale goes forward, it will be necessary to obtain consumer consent (with actual notice) before the records are sold/transferred in a bankruptcy proceeding. This CPO Report outlines for the Court's consideration the requirements and best practices for an Opt-In/Opt-Out process if a sale goes forward.[6]

Comprehensive privacy protections are provided in some U.S. state privacy and data protection laws, as well as the European Union (EU) General Data Protection Regulation (GDPR) and country privacy laws. The LPG privacy policy references and incorporates these far-reaching privacy protections for residents of California, as well as the 27 EU countries.

B. **Personal and Financial Data Collected and Maintained by LPG**

In the conduct of its business, LPG collected and maintained sensitive personal and financial data about tens of thousands of clients. The data collected by LPG makes privacy a particularly important factor in considering approval of any sale or transfer because the personal data is highly sensitive.

The LPG privacy policy details the types of personal and financial data the Debtor collected and maintains about consumers.

> **Categories of personal information collected, disclosed or sold**
>
> In this section we summarize the categories of personal information that we've collected, disclosed or sold and the purposes thereof. **You can read about these activities in detail in the section titled "Detailed information on the processing of Personal Data" within this document.**
>
> **Information we collect: the categories of personal information we collect**

[6] The Ombudsman has served as the CPO in 33 prior bankruptcy cases where privacy issues related to the sale of personal data were addressed. She has developed opt-in and opt-out processes in dozens of cases.

> We have collected the following categories of personal information about you: identifiers, commercial information and internet information.

The data includes personally identifiable information (PII) and confidential account numbers and financial records that must be protected.

The following client information is generally available in the LPG electronic record-keeping system (CRM). Client Name; Date of birth; Social Security Number; Phone Number; Email Address; Home Address; Debts enrolled; Bank Account information; Debit Card information; Signed Retainer Agreement. The Privacy Policy states that LPG may have also created additional personal data items ("private profiles") by matching the PII of clients with publicly available information.

This is all the personal and financial data a criminal or unscrupulous individual would need to engage in fraud, theft or identify theft of the vulnerable consumers in this case. As many as 40,000 of them were enticed to sign contracts that violate federal and state laws. The privacy of the ~ 40,000 LPG clients must be protected and their PII and bank account information cannot be sold or transferred to a company or individuals who are not acting in compliance with the law.

Further, the heightened risk of data breaches of consumer data should be a paramount concern, because small companies, and particularly lawyers, have been targeted by hackers. Minimizing the amount of personal data collected, maintained, and sold by companies is one of the most effective ways to protect it from data breaches. In the past few years, these breaches have occurred with alarming frequency. Millions of personal and financial records have been stolen and huge losses to the companies and their investors have resulted. If consumer data falls into the wrong hands, there is a vibrant black market for stolen personal data, often posted on the dark web, and the risk of identity theft and fraud has increased dramatically.

A critical first step is for the Court to order an accounting of all the client records, including client files that have been shared with or transferred to other individuals and entities without the consent of the consumers. The Court has ordered that the pre-petition transfer of 40,000 customer files to Phoenix Law was avoidable and recoverable transfer(s). Phoenix will return the files to the Debtor. [Doc. No. 176, filed 7/6/23]. Were consumer files transferred without authorization to CLG?

Practical steps the parties have taken in prior bankruptcy cases to protect the privacy of personal data involve creating a targeted sale that included only the consumers' records required for the particular business purposes and requirements of the Purchaser, and offering consumers notice of the sale and providing an opportunity to Opt-in[7] or Opt-out of having their personal and financial records transferred to the Purchaser.[8]

Those records not sold included data about children,[9] financial data (credit card numbers and bank and tax records),[10] dating site records of encounters and personal communications,[11] records of books and videos purchased,[12] subscribers to XY, a gay male youth-oriented magazine,

[7] Opt-in" consent requires affirmative steps by a consumer to allow the collection and/or use of Personally Identifiable Information; "Opt-out" consent requires affirmative steps to prevent the collection and/or use of Personally Identifiable Information. The determination of whether an Opt-in or an Opt-out process should be followed is based on data sensitivity; an Opt-in process is usually appropriate for the sale of the most sensitive consumer data such as bank records and other types of financial information.

[8] This approach is consistent with FTC recommendations in prior bankruptcy cases to limit the amount of data in the sales. For example, in the Borders bankruptcy case, the FTC recommended that any transfer of personal information take place only with the consent of Border's customers or with significant restrictions on the transfer and use of the information. *In re* Borders Group, Inc., No. 11-10614-mg (Bankr. S.D.N.Y.) (Glenn, J.) FTC Seeks Protection for Personal Customer Information in Borders Bankruptcy Proceeding, (Sep. 21, 2011), https://www.ftc.gov/news-events/news/press-releases/2011/09/ftc-seeks-protection-personal-customer-information-borders-bankruptcy-proceeding.

[9] *In re* Toysmart, *supra* note 12.

[10] Numerous cases, including *In re* JK Harris & Co. No. 2:11-bk-06254 (Bankr. D. SC) (Waites, J.).

[11] *In re* True Beginnings, No. 4:12-bk-42061 (ED TX) (Rhoades, J.)

[12] *In re* Borders Group, Inc., *supra* note 15.

including photos and online profiles,[13] demographic data (racial/ethnic, age, children, household members' income and education),[14] patient healthcare records,[15] medical records[16] and genetic data,[17] details of retail transactions,[18] and multiple copies of personal data on backup media.[19]

C. The LPG Case in Context

The Federal Trade Commission (FTC) has brought scores of law enforcement actions against credit-related services, and the agency has partnered with the states to bring hundreds of additional lawsuits.[20]

This LPG record is replete with complaints about the operations of LPG and objections to the potential sale of the consumer records. In a letter dated July 13, 2023 to U.S. Trustee Peter Anderson, the Consumer Financial Protection Bureau (CFTC), the federal agency responsible for enforcing federal consumer protection laws, stated that the "descriptions of LPG's business model and resulting consumer harm are echoed in hundreds of consumer complaints." "Numerous other consumers have alleged that LPG took upfront fees for debt relief without providing any services." The letter details a number of legal concerns about the potential sale.

---

[13] *In re* Peter Ian Cummings, Case No. 10-14433 (Bankr. D. N.J.) (Kaplan, J.) An FTC letter requested that the data be destroyed, suggesting the sale could violation the FTC Act prohibition against unfair or deceptive acts or practices. https://www.ftc.gov/system/files/documents/closing_letters/letter-xy-magazine-xy.com-regarding-use-sale-or-transfer-personal-information-obtained-during-bankruptcy-proceeding/100712xy.pdf.

[14] *In re* QSL of Medina, No. 15-52722 (Bankr. ND NY) (Koschik, J.)

[15] *In re* NovaSom, No. 19-11734 (BLS) (Bankr. D DE) (Shannon, J.)

[16] *In re* Laboratory Partners, No. 1:13-bk-12769 (Bankr. D.Del.) (Silverstein, J.)

[17] *In re* deCODE Genetics, No. 09-14063 (Bankr. D.Del.) (Silverstein, J.)

[18] *In re* Circuit City, No. 3:08-bk-35653 (Bankr. E.D.Va.) (Huennekens, J.)

[19] *In re* Linens N Things, 08-10832 (CSS) (D DE) (Sontchi, J.)

[20] Federal Trade Commission, Debt Relief Services & the Telemarketing Sales Rule: A Guide for Business, available at https://www.ftc.gov/business-guidance/resources/debt-relief-services-telemarketing-sales-rule-guide-business.

The U.S. Trustee has received letters from the California Department of Financial Protection and Innovation ("DFPI"), the Office of Attorney General for the Commonwealth of Pennsylvania ("PA-AG"), and the Office of Attorney General for New York ("NY-AG") raising concerns about LPG's operation and the proposed sale. Letters attached to U.S. Trustee's Response to Order Re Additional Briefing Sale Motion [Doc. No. 259, filed. 7/17/23]

The Attorney General of the Commonwealth of Pennsylvania concluded in a letter dated July 17, 2023 that after a review of complaints received they "preliminarily indicate that LPG has engaged in a pattern of unfair and deceptive acts and practices in the Commonwealth of Pennsylvania." "The Commonwealth is concerned that the proposed sale will allow for the continuation of these unfair and deceptive practices to the financial detriment of Pennsylvania consumers. *Most importantly, Consumer Legal Group, P.C. ("CLG"), the proposed buyer, is not licensed to provide debt settlement services in Pennsylvania* and it is unknown whether CLG is properly licensed and bonded to ensure adequate consumer protection." Similarly, the Attorney General of New York expressed concerns about the Consumer Law Group, a New York company created in 2022.

As an indication of how widespread the concerns have become, Google instituted a ban on paid credit repair services ads.[21] In November 2019 Google announced that it would update its policies to restrict the advertisement of credit repair services. Since then, paid ads for credit repair services are no longer allowed. This policy applies globally to all accounts that advertised credit repair services directly, to lead generators, and to those who connect consumers with third-party services.

[21] Google Update to Financial products and services policy (Nov. 2019), https://support.google.com/adspolicy/answer/9508775?hl=en.

Developments regarding PGX Holdings. PGX is a private technology and services company based in Salt Lake City, Utah that specializes in credit report repair services and consumer credit education.[22]

CFPB Enforcement Action. On May 2, 2019, the CFPB filed a five count complaint against several PGX entities and the Lexington Law Firm. *Bureau of Consumer Financial Protection v. Progrexion Marketing, Inc.*, *et al*., Case No. 2:19-CV-00298-BSJ (U.S. D.C. D. Utah).

On March 10, 2023, the District Court granted a partial summary judgment against the Debtors on Count I, finding in favor of the CFPB and holding that the Debtor defendants violated the advance fee provision of the Telemarketing Services Rule (TSR). The Court is currently considering the CFPB's Motion for Award of Monetary and Injunctive Relief, which seeks, among other things, prospective injunctive relief enjoining future violations of the advance fee provision and over $2.7 billion in monetary relief. Counts II-V allege various unlawful deceptive acts or practices.

Operational Restructuring Efforts in Response to the CFPB Litigation: PGX shut down call center operations. Fallout from the partial summary judgment ruling was significant. The company immediately stopped all telemarketing, closed call centers, and instituted a review of billing practices and mass consumer marketing across their businesses. It laid off approximately 900 employees. PGX Holdings, Wallace Decl. *supra,* para 29, page 14.

Bankruptcy Filing. On June 4, 2023, the PBX Debtors filed voluntary petitions under chapter 11 of the Bankruptcy Code in Delaware. A hearing to consider approval of the bid procedures is scheduled for July 31, 2023.

[22] *In re* PGX Holdings, Inc., et al., Case No. 23-10718 (CTG), Declaration Of Chad Wallace, Chief Executive Officer of PGX Holdings, Inc. in Support of Debtors' Chapter 11 Petitions and First Day Motions [ECF No. 12, filed 6/4/23].

II. The Sale or Transfer Must Not Violate Applicable Non-Bankruptcy Laws

Section 363(b)(1) of the Bankruptcy Code provides that the sale may not violate any of the following non-bankruptcy laws.

1. Telemarketing Sales Rule

The Telemarketing Sales Rule (TSR) has covered a wide variety of telemarketing transactions since it was enacted in 1995, including the sale of credit repair services, products with a negative option feature, prize promotions and advance fee loans. Debt relief companies that initiate calls to potential customers or hire others to call people for them have always been covered by the TSR.

In 2010, the FTC amended its TSR to protect consumers seeking debt relief services such as debt settlement or credit counseling. The Rule prohibits for-profit companies that sell these services over the telephone from charging a fee before they actually settle or reduce a consumer's debt. It also prohibits debt relief providers from making misrepresentations and requires that they disclose key information that consumers need in evaluating these services.

2. **Fair Debt Collection Practices Act** (FDCPA)

The FDCPA provides that a debt collector is not allowed to use unfair practices to collect a debt. In addition, there are state and other federal laws that generally prohibit practices that might be considered unfair, deceptive, or abusive acts or practices. The CFPB issued “rules” effective on November 30, 2021 that clarify and interpret the federal FDCPA.

3. **Federal Credit Repair Organizations Act** (CROA)

This Act, Title IV of the Consumer Credit Protection Act, prohibits untrue or misleading representations and requires certain affirmative disclosures in the offering or sale of "credit repair" services. The Act bars companies offering credit repair services from demanding advance

payment, requires that credit repair contracts be in writing, and gives consumers certain contract cancellation rights.

Both the federal Credit Repair Organizations Act (CROA), 15 U.S.C. §§ 1679 et al., and New York's GBL Article 28-BB prohibit the charging of upfront fees by credit repair organizations and credit services businesses and require certain disclosures. See 15 U.S.C. §§ 1679b(b); 1679c & 1679d; GBL §§ 458-e, 458-f & 458-d.0F.

Similarly, both federal and New York law protect consumers from deceptive and abusive telemarketing schemes. See 16 C.F.R. § 310, et seq. ("TSR") and New York GBL § 399-pp, et seq. These laws prohibit sellers or telemarketers from engaging in deceptive practices, 16 C.F.R. § 310.3; GBL § 399-pp(1), and from charging advance fees for certain services, including credit repair services (for both the federal and state statutes) or debt relief services (for the federal statute only). 16 C.F.R. § 310.4(a)(2) (prohibiting upfront fees for credit repair); GBL § 399-pp(6)(a)(9) (same); 16 C.F.R. § 310.4(a)(5) (prohibiting upfront fees for debt relief).

Thus, to be in compliance with the state and federal credit repair organizations acts and the telemarketing sales rules, a debt settlement company in New York cannot charge fees until it has resolved or settled the consumer's debt or repaired the consumer's credit.

4. Unfair, Deceptive, or Abusive Acts and Practices (UDAAP)

The FTC and CFPB have unique powers to protect consumers against "unfair" and "deceptive" acts and practices—with the CFPB also having additional powers to address "abusive" acts and practices. Those broad enforcement authorities encompass the key areas of fraud protection and consumer privacy with respect to digital assets. Unfair, deceptive, or abusive acts and practices (UDAAP) can cause significant financial injury to consumers, erode consumer confidence, and undermine the financial marketplace.

The CFPB regulates the offering of consumer financial products and services under the federal consumer financial laws, including (among others) the Dodd-Frank Act's prohibition against unfair, deceptive, or abusive acts or practices for consumer financial products and services. The CFPB has supervisory authority for detecting and assessing risks to consumers and to markets for consumer financial products and services.

Recent interpretations of federal law provide examples of what may constitute an unfair, deceptive, or abusive act or practice. The *Joint Statement on Crypto-Asset Risks to Banking Organizations* provides the opinion of the three federal banking agencies that "[i]naccurate or misleading representations and disclosures by crypto-asset companies, including misrepresentations regarding federal deposit insurance, and other practices that may be unfair, deceptive, or abusive," are contributing to significant harm to retail and institutional investors, customers, and counterparties.[23]

Inadequate security for the sensitive consumer information collected, processed, maintained, or stored by the company can constitute an unfair practice in violation of 12 U.S.C. 5536(a)(1)(B). Guidance issued by the CFPB with respect to the adequacy of cybersecurity provides an instructive interpretation of UDAAP under the Dodd-Frank Act:[24]

> Acts or practices are unfair when they cause or are likely to cause substantial injury that is not reasonably avoidable or outweighed by countervailing benefits to consumers or competition. Inadequate authentication, password management, or software update policies or practices are likely to cause substantial injury to consumers that is not reasonably avoidable by consumers, and financial institutions are unlikely to successfully justify weak data security practices based on countervailing benefits to consumers or competition. Inadequate data security can be an unfair practice in the absence of a breach or intrusion."

---

[23] https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20230103a1.pdf.

[24] CFPB, Consumer Financial Protection Circular 2022-04, https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/.

Section 5(a) of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. Sec. 45(a)(1).[25] An act or practice is unfair if (1) it causes or is likely to cause substantial injury, (2) the injury is not reasonably avoidable by consumers, and (3) the injury is not outweighed by benefits to consumers or competition. 15 U.S.C. Sec. 45(n). "Deceptive" practices are defined in the Commission's Policy Statement on Deception[26] as involving a material representation, omission or practice that is likely to mislead a consumer acting reasonably in the circumstances. The FTC has brought many cases alleging that the failure to adhere to promises about privacy constitute a deceptive practice under the FTC Act.

"Unfair business practices" is an evolving concept reflecting the ingenuity of unscrupulous business persons in concocting new schemes to gain advantage at someone else's expense. The FTC has identified several factors to be considered in determining whether a practice is unfair. The injury must be substantial, outweigh any countervailing benefit to the consumer, and be one the consumer cannot reasonably avoid.

With respect to privacy, the FTC has adopted widely-accepted principles concerning fair information practices[27] and enforces laws prohibiting unfair and deceptive practices. This include cases against companies that make false or misleading statements in their privacy policies. Under Section 5, the FTC has pursued privacy and data security cases in myriad areas, including against

[25] FTC *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority* (May 2021), https://www.ftc.gov/about-ftc/mission/enforcement-authority. FTC *Report to Congress on Privacy and Security* (Sep. 13, 2021), https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf.

[26] See FTC Policy Statement on Deception (Oct. 23, 1984) (appended to *Cliffdale Assocs., Inc.,* 103 F.T.C. 110, 183 (1984)), https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.

[27] FTC Report—*Privacy Online: Fair Information Practices in the Electronic Marketplace*, www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

social media companies, mobile app developers, data brokers, ad tech industry participants, retailers, and companies in the Internet of Things space.

5. Privacy of Consumer Financial Information

Some governments—such as California and the European Union (EU)—have recently enacted privacy laws regulating nearly all forms of personal data within their jurisdictional reach. In the U.S. federal privacy laws are sector-specific and many privacy protections are provided in state laws. In addition, the Debtor and the Purchaser must abide by the European Union and country laws when processing, transferring or disposing of the data of consumers who reside in those jurisdictions.

Federal law protects financial information, including credit card numbers, and provides certain requirements for providing notice of an organization's privacy policy and an opportunity for consumers to opt-out of changes to that policy.

6. State Laws – Unfair and Deceptive Practices (UDP)

As with Section 5 of the FTC Act, states have enacted their own consumer protection laws that similarly prohibit unfair and deceptive acts or practices.[28] Many state laws also prohibit unfair or unconscionable practices, and a few prohibit abusive practices.

All 50 states have Unfair and Deceptive Acts and Practices (UDAP) laws that have been used to bring cases against companies that have false or misleading statements in their privacy policies posted online.

7. State Laws Related to Digital Privacy[29]

[28] Carolyn Carter, Consumer Protection in the States: A 50-State Evaluation of Unfair and Deceptive Practices Laws (2018), NATIONAL CONSUMER LAW CENTER, https://www.nclc.org/resources/how-well-do-states-protect-consumers/. Appendix A – Capsule Summaries Of Strengths And Weaknesses Of Each State's UDAP Statute.

[29] National Conference of State Legislatures (NCSL), State Laws Related to Digital Privacy (updated June 7, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-

Because the U.S. does not have a comprehensive federal privacy law, several U.S. states have created their own privacy laws. These laws afford specific protections to individuals and place clear obligations on businesses that collect and use personal data. Five states have enacted comprehensive consumer privacy laws:[30]

- California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100 et seq.) and California Consumer Privacy Rights Act, 2020 (Proposition 24)
- Virginia Consumer Data Protection Act, 2021 H.B. 2307|2021 S.B. 1392 (Effective Jan. 1, 2023.)
- Colorado Privacy Act, 2021 S.B. 190 (Effective July 1, 2023.)
- Connecticut 2022 S.B. 6 (Personal Data Privacy and Online Monitoring) (Effective July 1, 2023.)
- Utah Consumer Privacy Act, 2022 S.B. 227 (Effective Dec. 31, 2023.)

California Privacy Protection Act (CCPA)[31]

The CCPA gives consumers more control over the personal information that businesses collect about them. This law secures privacy rights for California consumers, including:

- The right to know about the personal information a business collects about them and how it is used and shared;
- The right to delete personal information collected from them (with some exceptions);
- The right to opt-out of the sale of their personal information.

Businesses are required to give consumers certain notices explaining their privacy practices.

---

privacy.aspx; NCSL 2022 Consumer Privacy Legislation (June 10, 2022), https://www.ncsl.org/about-state-legislatures/2022-consumer-privacy-legislation.

International Association of Privacy Professionals (IAPP), US State Privacy Legislation Tracker 2022, Comprehensive Consumer Privacy Bills, https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf

[30] *See*, IAPP, *US State Privacy Legislation* Tracker (updated Oct. 7, 2022), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

[31] State of California Department of Justice, Xavier Becerra, Attorney General, https://oag.ca.gov/privacy/ccpa

Limitations are imposed on the sale or transfer of Personally Identifiable Information by the California Consumer Privacy Act of 2018 ("CCPA") (Cal. Civ. Code §§ 1798.100-1798.199), as amended, and expanded by the California Privacy Rights Act (effective as of January 1, 2023). Cal. Code Regulation Title 11, §7013(e).

A business that sells or shares the personal information of consumers shall provide the Notice of Right to Opt-out of Sale/Sharing to consumers as follows:

(1) A business shall post the Notice of Right to Opt-out of Sale/Sharing on the internet webpage to which the consumer is directed after clicking on the "Do Not Sell or Share My Personal Information" link. The notice shall include the information specified in subsection (f) or be a link that takes the consumer directly to the specific section of the business's privacy policy that contains the same information. If clicking on the "Do Not Sell or Share My Personal Information" link immediately effectuates the consumer's right to opt-out of sale/sharing or if the business processes opt-out preference signals in a frictionless manner and chooses not to post a link, the business shall provide the notice within its privacy policy.

(2) A business that does not operate a website shall establish, document, and comply with another method by which it informs consumers of their right to opt-out of sale/sharing. That method shall comply with the requirements set forth in section 7003.

(3) A business shall also provide the notice to opt-out of sale/sharing in the same manner in which it collects the personal information that it sells or shares. Illustrative examples follow.

(4) A business that sells or shares personal information that it collects in the course of interacting with consumers offline, such as in a brick-and-mortar store, shall provide notice through an offline method, *e.g.*, on the paper forms that collect the personal information or by posting signage in the area where the personal information is collected directing consumers to where the notice can be found online.

(5) A business that sells personal information that it collects over the phone shall provide notice orally during the call when the information is collected.

8. State Data Breach Notification Laws and Data Protection Provisions

All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted data breach notification laws that require any business in possession of certain sensitive personal information about a covered individual to disclose a security breach of that information

to the person(s) affected.[32] State Attorneys General are enforcing a variety of the consumer protection, data breach notification laws and data disposal that are relevant in bankruptcy cases.

A number of states require companies that maintain certain personal information of state residents to take steps to protect against data breaches through data security measures, as well as secure disposal of personal information. At least 24 states have laws that address data security practices of private sector entities. Most of these data security laws require businesses to implement and maintain "reasonable security procedures and practices" appropriate to the nature of the information and to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.[33]

Below are examples of specific security requirements in the laws of states where large numbers of LPG customers are located:

- ***California*** – Data custodians must implement reasonable security procedures and practices.
- ***Florida*** – Requires "reasonable measures to protect and secure data in electronic form containing personal information."[34]
- ***New York –*** Companies must develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of private information including, but not limited to, disposal of data.[35]

[32] NCSL Security Breach Notification Laws, *available at* https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[33] NCSL, Data Security Laws, Private Sector (May 29, 2019), *available at* https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

[34] Florida Information Protection Act of 2014 (SB 1524) (Fla. Stat. § 501.171).

[35] New York Gen. Bus. Law s 899-BB; data breach notification N.Y. Gen. Bus. Law § 899-AA.

9. State Data Disposal Laws

At least 35 states and Puerto Rico have laws that govern the disposal of personal data held by businesses.[36] The laws, that require persons or entities to destroy, dispose of, or otherwise make personal information unreadable or undecipherable, will protect the privacy of LPG clients. For example, Section 399-H of the New York General Business Law provides that a person or entity must dispose of materials containing personal information in a manner "consistent with commonly accepted industry practices that it reasonably believes will ensure that no unauthorized person will have access to the personal identifying information contained in the record."[37]

Privacy Laws of the European Union[38] and Country Laws

More than 120 countries have privacy laws for data protection to ensure that citizens and their data are offered rigorous protections and controls.[39]

1. European Union (EU) General Data Protection Regulation (GDPR)

The European Union (EU) GDPR[40] contains requirements related to consumer consent, mandatory data breach notification, and data management and portability. The law mandates that all businesses with European customers must fully adopt GDPR principles, including an adequate security strategy and technical measures to protect the personal data of EU citizens.

---

[36] *See* NCLS, Data Disposal Laws, https://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

[37] N.Y. Gen. Bus. Law § 399-H.

[38] The 27 EU countries are Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.

[39] IAPP Global Comprehensive Privacy Law Mapping Chart (April 2022), https://iapp.org/media/pdf/resource_center/global_comprehensive_privacy_law_mapping.pdf; Online Consumer Protection Legislation Worldwide, United National Conference on Trade and Development (UNCTAD), https://unctad.org/page/online-consumer-protection-legislation-worldwide.

[40] *See* GDPR Portal, *available at* https://www.eugdpr.org/.

The six GDPR data protection principles are: (1) Lawfulness, fairness and transparency; (2) Purpose limitation; (3) Data minimization; (4) Accuracy; (5) Storage limitation; and (6) Integrity and confidentiality.

The GDPR has an extra-territorial effect. The Directive applies to all companies processing the personal data[41] of data subjects residing in the EU, regardless of the company's location. The GDPR also applies to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behavior that takes place within the EU.

2. Country Privacy Laws

The laws and regulations that address personal data protection vary significantly from region to region or even country to country.[42] As more and more social and economic activities take place online, the importance of privacy and data protection is increasingly recognized. Of equal concern is the collection, use and sharing of personal information to third parties without notice or consent of consumers. 137 out of 194 countries have put in place legislation to secure the protection of data and privacy.

III. Recommendations and Conclusions

A. "Qualified Buyer" Criteria – Developed in Prior Bankruptcy Cases

While asset sales are conducted to maximize the value of the estate and the return to creditors, the Bankruptcy Code also recognizes the importance of protecting the privacy of the

[41] Any information related to a natural person or 'data subject' that can be used to directly or indirectly identify the person, including a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

[42] UNCTAD, Data Protection and Privacy Legislation Worldwide, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

personal data of individual consumers. Thus due diligence is essential to ensure that the proposed Purchaser(s) have demonstrated the capability to protect the privacy of the records of LPG clients and the intention to abide by an appropriate privacy policy.

To that end, over the years since the privacy requirements of the Bankruptcy Code were enacted in 2005, Bankruptcy Courts have applied certain criteria to establish that a Purchaser is "qualified" and would protect the privacy of the consumer data it purchased.[43] The FTC reiterated the applicability of these conditions in the Radio Shack bankruptcy case.[44]

The CPO recommends that the following "Qualified Buyer" criteria apply to the proposed Purchaser(s).

- **The Purchaser is in the same line of business as the Debtor.**

There is more to a finding of "qualified buyer" than merely the nature of the bidder's business—due diligence includes an understanding of a potential Purchaser's background. In this case, due diligence should be conducted to evaluate the Consumer Legal Group and any other prospective bidders if the Court orders that an auction will be conducted.

The Objections of Carolyn Beech and Diane Skarnavack to the Motion for Sale of Property of the Estate Under Section 363(b) (Doc. No. 185, filed 7/7/23] raises concerns about what work CLG performs and will perform for LPG clients, its capacity to represent clients in states across the country and the need to hire local council, the status of their existing contracts, what notice the

[43] *In re* Toysmart.com, *supra* note 11. *In re* Choxi, 16-13131 (SCC) (SD NY) (Chapman, J.); *In re* Century 21 Department Stores, 20-12097 (SD NY) (Chapman, J.); *In re* KB US Holding 20-22962 (SHL) (SD NY) (Lane, J); *In re* MKJC Hyundai, 20-42283, (SD NY) (Mazer-Marino, J.); *In re* Loot Crate, 19-11791-BLS (D DE) (Shannon, J.); *In re* NovaSom, 19-11734 (BLS) (D DE) (Shannon, J.); *In re* Hobbico, 18-10055 (KG) (D DE) (Gross J.); *In re* Circuit City Stores, 3:08-bk-35653 (ED VA) (Huennekens, J.); *In re* Coach Am Group Holdings, No. 12-10010 (KG) (Gross J.) (Bankr. D. Del.); *In re* Linens N Things, 08-10832 (CSS) (D DE) (Sontchi, J.).

[44] FTC Requests Bankruptcy Court Take Steps to Protect RadioShack Consumers' Personal Information. Letter to Consumer Privacy Ombudsman Describes Possible Conditions on Sale of Data (May 18, 2015), *In re* RadioShack Corporation, No. 15-10197 (BLS) (Bankr. D. Del.) (Shannon, J.), *available* https://www.ftc.gov/news-events/news/press-releases/2015/05/ftc-requests-bankruptcy-court-take-steps-protect-radioshack-consumers-personal-information.

clients should be provided concerning the effect of non-compliance with the Credit Repair Organization Act (CROA), the Fair Debt Collection Practices Act (FDCPA), and the fees the CLG plans to charge the clients. Beech asserts that "CLG's statements thus overstate both the benefits of its services and the need for them." Do the 40,000 LPG clients all need the services of a lawyer?

The due diligence process would evaluate whether the potential bidders have demonstrated expertise in operating a legitimate debt resolution business, and have experience handling large amounts of highly sensitive personal data and protecting it appropriately. Given the documented problems with some debt resolution companies, the proposed officers and directors should be scrutinized carefully, including conducting a criminal background check (audits, investigations, indictments and convictions). Assessing risks to consumers is critical because after the sale or transfer is approved, the Court has no authority to monitor the operations of the Purchaser.

- **The Purchaser agrees to use the personal consumer records for the same purpose(s) as they were used previously by LPG.**

This point addresses the well-established privacy principle that personal and financial consumer data should only be used for the same purpose(s) for which it was collected.

- **The Purchaser agrees to comply with an appropriate website privacy policy.**

This case would provide an excellent opportunity to develop a new privacy policy that reflects the legitimate business interests of the Purchaser and protects the privacy of consumers' data.

- **The Purchaser agrees that prior to making any "material change" to the privacy policy or using or disclosing personal information in a different manner from that specified in the privacy policy, it will notify consumers and afford them an opportunity to Opt-out of the changes to those policies or the new uses of their personal information.**
- **The Purchaser agrees to employ appropriate information security controls (technical,**

operational and managerial) to protect electronic personal and financial consumer information and encryption keys.

- **The Purchaser agrees to abide by all applicable federal, state, and international laws, including the debt resolution, privacy, data breach notification, data disposal, and cybersecurity laws and laws prohibiting unfair, deceptive or abusive practices "UDAP," "do-not-track," "do-not-call," and "no spam" laws.**

B. Consumer Consent – Opt-In and Opt-out Process

Providing notice and obtaining consumer consent are critical aspects of the bankruptcy sale process to protect the privacy of the sensitive personal and financial information LPG has collected and maintains. In a case such as this one, two types of consumer consent regimes should be considered: Opt-in and Opt-out. Opt-in regimes require affirmative steps by the consumer to allow the collection and/or use of his/her information. An Opt-in approach is usually appropriate for the sale or transfer of the most sensitive types of consumer data such as financial, tax, and medical records, and information about children.

If a sale is approved, the most sensitive personal and financial data may be included, although it would be preferable for the parties to agree on a targeted approach and include only the data the Purchaser needs to meet its legitimate business requirements. In addition, it will be necessary for the clients to sign new contracts with the Purchaser. Thus, actual notice is necessary and can be achieved through an Opt-in process. In many prior bankruptcy cases, the parties successfully adopted an Opt-in / Opt-out process designed to protect the privacy of all consumers to the greatest extent possible under the circumstances of the bankruptcy sale. The goal was to ensure that the process was transparent, meaningful and effective.

Recently, Trustee Richard Marshack sent a "Sale Email" to consumers[45] that provides notice of a potential sale in this case. The notice is helpful because it alerts clients to upcoming developments. However, a followup Opt-in process will need to be followed, as has been done in many prior bankruptcy cases, to provide the actual notice required.

The Opt-in must be designed to reach all consumers and all LPG clients must be accounted for. The notice should be sent after the conclusions of an auction and the successful bidder has been designated. It must provide to clients the name of the proposed Purchaser(s), identify and describe their organization and the services they offer, and include the new contract clients will be required to sign. Details related to all laws that apply, such as the right to stop withdrawals from a client's bank account, should be included.

The U.S. Trustee expressed concerns about the initial notice and offered recommendations that should be taken into account: "The Sale Email failed to alert the consumers that they must affirmatively "opt out" or they will be bound by the terms of the Modified Legal Services Agreement (attached as Exhibit "4" to the Declaration of Richard Marshack (in support of the Sale Motion). Further, the Sale Email informs consumers that they should "retain counsel" if they have an objection to the proposed sale. This is misleading because the consumers could file an objection to the Sale Motion even without an attorney. Further, the Trustee should include all pleadings relating to the Sale Motion, including the U.S. Trustee's Response and Opposition, to the DropBox available for all consumers to review to ensure that consumers can make an informed decision." [Doc. No. 259 page 13]

[45] The email (the "Sale Email") (attached as Exhibit "A" to the Sale Declaration) informs the consumers that they have "ninety (90) days from the date of the sale to either (1) "opt out" of further representation by the new law firm, recognizing that doing so will cancel your contract for services; or (2) you will be offered a new 'cured' contract with the new lawyers to be signed by you, and to allow for services to be performed on your behalf." Sale Declaration, at p. 7.

In the interests of providing customers with appropriate notice, the Ombudsman is available to work with the parties to draft the Opt-in notices. For clients who choose not to Opt-in, their information should be deleted from the LPG databases before any personal and financial data is transferred to the Purchaser.

Conclusion

The issues related to the sale or transfer of the personal and financial records of the 40,000 LPG consumers required under the Bankruptcy Code have been addressed, including compliance with the privacy policy, the application of non-bankruptcy laws, and the losses or gains, and costs or benefits to consumers, if the sale or transfer is approved.

The Ombudsman stands ready to answer any questions the Court and the parties may have, and confer with the parties to identify the privacy protections that should apply to the personal and financial data of the LPG consumers.

Respectfully submitted,

/s/ Lucy L. Thomson

Lucy L. Thomson
Consumer Privacy Ombudsman

APPENDIX A

Our Privacy Policy – Litigation Practice Group

[Archived copy; Latest update: August 30, 2021]

Privacy Policy of lpglaw.com

This Website collects some Personal Data from its Users.

This document contains a section dedicated to Californian consumers and their privacy rights.

This document can be printed for reference by using the print command in the settings of any browser.

Owner and Data Controller

Litigation Practice Group
17542 17th Street
Suite 100
Tustin CA 92780

Owner contact email: info@lpglaw.com

Types of Data collected

Among the types of Personal Data that this Website collects, by itself or through third parties, there are: Tracker; Usage Data; email address; first name; last name; phone number; ZIP/Postal code; device information; shopping history; unique device identifiers for advertising (Google Advertiser ID or IDFA, for example); various types of Data; address; Data communicated in order to use the Service.

Complete details on each type of Personal Data collected are provided in the dedicated sections of this privacy policy or by specific explanation texts displayed prior to the Data collection.

Personal Data may be freely provided by the User, or, in case of Usage Data, collected automatically when using this Website.

Unless specified otherwise, all Data requested by this Website is mandatory and failure to provide this Data may make it impossible for this Website to provide its services. In cases where this Website specifically states that some Data is not mandatory, Users are free not to communicate this Data without consequences to the availability or the functioning of the Service.

Users who are uncertain about which Personal Data is mandatory are welcome to contact the Owner.

Any use of Cookies – or of other tracking tools – by this Website or by the owners of third-party services used by this Website serves the purpose of providing the Service required by the User, in addition to any other purposes described in the present document and in the Cookie Policy, if available.

Users are responsible for any third-party Personal Data obtained, published or shared through this Website and confirm that they have the third party's consent to provide the Data to the Owner.

Mode and place of processing the Data

Methods of processing

The Owner takes appropriate security measures to prevent unauthorized access, disclosure, modification, or unauthorized destruction of the Data.

The Data processing is carried out using computers and/or IT enabled tools, following organizational procedures and modes strictly related to the purposes indicated. In addition to the Owner, in some cases, the Data may be accessible to certain types of persons in charge, involved with the operation of this Website (administration, sales, marketing, legal, system administration) or external parties (such as third-party technical service providers, mail carriers, hosting providers, IT companies, communications agencies) appointed, if necessary, as Data Processors by the Owner. The updated list of these parties may be requested from the Owner at any time.

Legal basis of processing

The Owner may process Personal Data relating to Users if one of the following applies:

- Users have given their consent for one or more specific purposes. Note: Under some legislations the Owner may be allowed to process Personal Data until the User objects to such processing ("opt-out"), without having to rely on consent or any other of the following legal bases. This, however, does not apply, whenever the processing of Personal Data is subject to European data protection law;
- provision of Data is necessary for the performance of an agreement with the User and/or for any pre-contractual obligations thereof;
- processing is necessary for compliance with a legal obligation to which the Owner is subject;
- processing is related to a task that is carried out in the public interest or in the exercise of official authority vested in the Owner;
- processing is necessary for the purposes of the legitimate interests pursued by the Owner or by a third party.

In any case, the Owner will gladly help to clarify the specific legal basis that applies to the processing, and in particular whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract.

Place

The Data is processed at the Owner's operating offices and in any other places where the parties involved in the processing are located.

Depending on the User's location, data transfers may involve transferring the User's Data to a country other than their own. To find out more about the place of processing of such transferred Data, Users can check the section containing details about the processing of Personal Data.

Users are also entitled to learn about the legal basis of Data transfers to a country outside the European Union or to any international organization governed by public international law or set up by two or more countries, such as the UN, and about the security measures taken by the Owner to safeguard their Data.

If any such transfer takes place, Users can find out more by checking the relevant sections of this document or inquire with the Owner using the information provided in the contact section.

Retention time

Personal Data shall be processed and stored for as long as required by the purpose they have been collected for.

Therefore:

- Personal Data collected for purposes related to the performance of a contract between the Owner and the User shall be retained until such contract has been fully performed.
- Personal Data collected for the purposes of the Owner's legitimate interests shall be retained as long as needed to fulfill such purposes. Users may find specific information regarding the legitimate interests pursued by the Owner within the relevant sections of this document or by contacting the Owner.

The Owner may be allowed to retain Personal Data for a longer period whenever the User has given consent to such processing, as long as such consent is not withdrawn. Furthermore, the Owner may be obliged to retain Personal Data for a longer period whenever required to do so for the performance of a legal obligation or upon order of an authority.

Once the retention period expires, Personal Data shall be deleted. Therefore, the right of access, the right to erasure, the right to rectification and the right to data portability

cannot be enforced after expiration of the retention period.

The purposes of processing

The Data concerning the User is collected to allow the Owner to provide its Service, comply with its legal obligations, respond to enforcement requests, protect its rights and interests (or those of its Users or third parties), detect any malicious or fraudulent activity, as well as the following: Remarketing and behavioral targeting, Analytics, Contacting the User, Advertising, Managing contacts and sending messages, User database management, Displaying content from external platforms, Infrastructure monitoring and Tag Management.

For specific information about the Personal Data used for each purpose, the User may refer to the section “Detailed information on the processing of Personal Data”.

Detailed information on the processing of Personal Data

Personal Data is collected for the following purposes and using the following services:

Advertising

This type of service allows User Data to be utilized for advertising communication purposes. These communications are displayed in the form of banners and other advertisements on this Website, possibly based on User interests.

This does not mean that all Personal Data are used for this purpose. Information and conditions of use are shown below.

Some of the services listed below may use Trackers to identify Users or they may use the behavioral retargeting technique, i.e. displaying ads tailored to the User’s interests and behavior, including those detected outside this Website. For more information, please check the privacy policies of the relevant services.

In addition to any opt-out feature offered by any of the services below, Users may opt out by visiting the Network Advertising Initiative opt-out page.

Users may also opt-out of certain advertising features through applicable device settings, such as the device advertising settings for mobile phones or ads settings in general.

Google Ad Manager (Google LLC)

Google Ad Manager is an advertising service provided by Google LLC that allows the Owner to run advertising campaigns in conjunction with external advertising networks that the Owner, unless otherwise specified in this document, has no direct relationship with. In order to opt out from being tracked by various advertising networks, Users may make use of Youronlinechoices. In order to understand Google’s use of data, consult Google’s partner policy.

This service uses the “DoubleClick” Cookie, which tracks use of this Website and User behavior concerning ads, products and services offered.
Users may decide to disable all the DoubleClick Cookies by going to: Google Ad Settings.
Personal Data processed: Tracker; Usage Data.
Place of processing: United States – Privacy Policy.
Category of personal information collected according to CCPA: internet information.
This processing constitutes a sale based on the definition under the CCPA. In addition to the information in this clause, the User can find information regarding how to opt out of the sale in the section detailing the rights of Californian consumers.

LinkedIn Ads (LinkedIn Corporation)

LinkedIn Ads is an advertising service provided by LinkedIn Corporation.
Personal Data processed: Tracker; Usage Data.
Place of processing: United States – Privacy Policy – Opt out.
Category of personal information collected according to CCPA: internet information.
This processing constitutes a sale based on the definition under the CCPA. In addition to the information in this clause, the User can find information regarding how to opt out of the sale in the section detailing the rights of Californian consumers.

NextRoll (NextRoll, Inc.)

NextRoll is an advertising service provided by NextRoll, Inc. NextRoll, Inc. performs a hash of the User’s email address in order to serve targeted advertising to other devices connected to them (i.e. cross-device tracking).
Personal Data processed: device information; purchase history; Tracker; unique device identifiers for advertising (Google Advertiser ID or IDFA, for example); Usage Data.
Place of processing: United States – Privacy Policy – Opt Out.
Category of personal information collected according to CCPA: identifiers; commercial information; internet information.
This processing constitutes a sale based on the definition under the CCPA. In addition to the information in this clause, the User can find information regarding how to opt out of the sale in the section detailing the rights of Californian consumers.

Analytics

The services contained in this section enable the Owner to monitor and analyze web trac and can be used to keep track of User behavior.

Google Analytics (Google LLC)

Google Analytics is a web analysis service provided by Google LLC (“Google”). Google utilizes the Data collected to track and examine the use of this Website, to prepare reports

on its activities and share them with other Google services.
Google may use the Data collected to contextualize and personalize the ads of its own advertising network.
Personal Data processed: Tracker; Usage Data.
Place of processing: United States – Privacy Policy – Opt Out.
Category of personal information collected according to CCPA: internet information.
This processing constitutes a sale based on the definition under the CCPA. In addition to the information in this clause, the User can find information regarding how to opt out of the sale in the section detailing the rights of Californian consumers.

Google Analytics with anonymized IP (Google LLC)

Google Analytics is a web analysis service provided by Google LLC (“Google”). Google utilizes the Data collected to track and examine the use of this Website, to prepare reports on its activities and share them with other Google services.
Google may use the Data collected to contextualize and personalize the ads of its own advertising network.
This integration of Google Analytics anonymizes your IP address. It works by shortening Users’ IP addresses within member states of the European Union or in other contracting states to the Agreement on the European Economic Area. Only in exceptional cases will the complete IP address be sent to a Google server and shortened within the US.
Personal Data processed: Tracker; Usage Data.
Place of processing: United States – Privacy Policy – Opt Out.
Category of personal information collected according to CCPA: internet information.
This processing constitutes a sale based on the definition under the CCPA. In addition to the information in this clause, the User can find information regarding how to opt out of the sale in the section detailing the rights of Californian consumers.

Contacting the User

Mailing list or newsletter (this Website)

By registering on the mailing list or for the newsletter, the User’s email address will be added to the contact list of those who may receive email messages containing information of commercial or promotional nature concerning this Website. Your email address might also be added to this list as a result of signing up to this Website or after making a purchase.
Personal Data processed: email address; rst name; last name; phone number; ZIP/Postal code.
Category of personal information collected according to CCPA: identifiers.

Displaying content from external platforms

This type of service allows you to view content hosted on external platforms directly from the pages of this Website and interact with them.

This type of service might still collect web trac data for the pages where the service is installed, even when Users do not use it.

YouTube IFrame Player (Google LLC)

YouTube IFrame Player is a video content visualization service provided by Google LLC that allows this Website to incorporate content of this kind on its pages.

Through this Service, this Website may collect Data directly or indirectly on or from Users' devices, including by making use of trackers. Users may restrict such access to their Data via the security settings page provided by Google. Users may ask the Owner for further information about these privacy settings at any time through the contact details provided in this document.

Data collected through the Service may also be used to help third parties deliver interest-based advertising. Users can opt out of third-party interest-based advertising through their device settings or by visiting the Network Advertising Initiative opt-out page.

Personal Data processed: Data communicated in order to use the Service.

Place of processing: United States – Privacy Policy – Opt out.

Category of personal information collected according to CCPA: internet information.

This processing constitutes a sale based on the definition under the CCPA. In addition to the information in this clause, the User can find information regarding how to opt out of the sale in the section detailing the rights of Californian consumers.

Google Fonts (Google LLC)

Google Fonts is a typeface visualization service provided by Google LLC that allows this Website to incorporate content of this kind on its pages.

Personal Data processed: Usage Data; various types of Data as specified in the privacy policy of the service.

Place of processing: United States – Privacy Policy.

Category of personal information collected according to CCPA: internet information.

This processing constitutes a sale based on the definition under the CCPA. In addition to the information in this clause, the User can find information regarding how to opt out of the sale in the section detailing the rights of Californian consumers.

Font Awesome (Fonticons, Inc.)

Font Awesome is a typeface visualization service provided by Fonticons, Inc. that allows this Website to incorporate content of this kind on its pages.

Personal Data processed: Usage Data.

Place of processing: United States – Privacy Policy.

Category of personal information collected according to CCPA: internet information.

This processing constitutes a sale based on the definition under the CCPA. In addition to the information in this clause, the User can find information regarding how to opt out of the sale in the section detailing the rights of Californian consumers.

Infrastructure monitoring

This type of service allows this Website to monitor the use and behavior of its components so its performance, operation, maintenance and troubleshooting can be improved.

Which Personal Data are processed depends on the characteristics and mode of implementation of these services, whose function is to filter the activities of this Website.

Rollbar (Rollbar, Inc.)

Rollbar is a monitoring service provided by Rollbar, Inc.

Personal Data processed: various types of Data as specified in the privacy policy of the service.

Place of processing: United States – Privacy Policy.

Category of personal information collected according to CCPA: internet information.

Managing contacts and sending messages

This type of service makes it possible to manage a database of email contacts, phone contacts or any other contact information to communicate with the User.

These services may also collect data concerning the date and time when the message was viewed by the User, as well as when the User interacted with it, such as by clicking on links included in the message.

AdRoll Email (NextRoll, Inc.)

AdRoll Email is an email address management and message sending service provided by NextRoll, Inc. NextRoll, Inc. performs a hash of the User's email address in order to serve targeted advertising to other devices connected to them (i.e. cross-device tracking).

Users can opt-out of receiving interest-based ads by visiting the Adroll opt-out page, following the instructions provided by the Network Advertising Initiative or directly through their device advertising settings.

Personal Data processed: first name; last name.

Place of processing: United States – Privacy Policy – Opt Out.

Category of personal information collected according to CCPA: identifiers.

This processing constitutes a sale based on the definition under the CCPA. In addition to the information in this clause, the User can find information regarding how to opt out of

the sale in the section detailing the rights of Californian consumers.

ZOHO Campaigns (Zoho Corporation Pvt. Ltd.)

ZOHO Campaigns is an email address management and message sending service provided by Zoho Corporation Pvt. Ltd.

Personal Data processed: rst name; last name.

Place of processing: United States – Privacy Policy.

Category of personal information collected according to CCPA: identifiers.

This processing constitutes a sale based on the definition under the CCPA. In addition to the information in this clause, the User can nd information regarding how to opt out of the sale in the section detailing the rights of Californian consumers.

Remarketing and behavioral targeting

This type of service allows this Website and its partners to inform, optimize and serve advertising based on past use of this Website by the User.

This activity is facilitated by tracking Usage Data and by using Trackers to collect information which is then transferred to the partners that manage the remarketing and behavioral targeting activity.

Some services offer a remarketing option based on email address lists.

In addition to any opt-out feature provided by any of the services below, Users may opt out by visiting the Network Advertising Initiative opt-out page.

Users may also opt-out of certain advertising features through applicable device settings, such as the device advertising settings for mobile phones or ads settings in general.

Google Ads Remarketing (Google LLC)

Google Ads Remarketing is a remarketing and behavioral targeting service provided by Google LLC that connects the activity of this Website with the Google Ads advertising network and the DoubleClick Cookie.

Users can opt out of Google’s use of cookies for ads personalization by visiting Google’s Ads Settings.

Personal Data processed: Tracker; Usage Data.

Place of processing: United States – Privacy Policy – Opt Out.

Category of personal information collected according to CCPA: internet information.

This processing constitutes a sale based on the definition under the CCPA. In addition to the information in this clause, the User can find information regarding how to opt out of the sale in the section detailing the rights of Californian consumers.

AdRoll (NextRoll, Inc.)

AdRoll is an advertising service provided by NextRoll, Inc. AdRoll can serve targeted advertising on any device connected to the User, by processing their email address **using a security technique called hashing.**

AdRoll may also automatically collect certain types of data to serve personalized recommendations to the User, as stated in its privacy policy.

Personal Data processed: device information; shopping history; Tracker; unique device identifiers for advertising (Google Advertiser ID or IDFA, for example); Usage Data; various types of Data.

Place of processing: United States – Privacy Policy – Opt Out.

Category of personal information collected according to CCPA: identifiers; commercial information; internet information.

This processing constitutes a sale based on the denition under the CCPA. In addition to the information in this clause, the User can nd information regarding how to opt out of the sale in the section detailing the rights of Californian consumers.

Facebook Custom Audience (Facebook, Inc.)

Facebook Custom Audience is a remarketing and behavioral targeting service provided by Facebook, Inc. that connects the activity of this Website with the Facebook advertising network.

Users can opt out of Facebook's use of cookies for ads personalization by visiting this opt-out page.

Personal Data processed: email address; Tracker.

Place of processing: United States – Privacy Policy – Opt Out.

Category of personal information collected according to CCPA: identifiers; internet information.

This processing constitutes a sale based on the definition under the CCPA. In addition to the information in this clause, the User can find information regarding how to opt out of the sale in the section detailing the rights of Californian consumers.

Tag Management

This type of service helps the Owner to manage the tags or scripts needed on this Website in a centralized fashion.

This results in the Users' Data owing through these services, potentially resulting in the retention of this Data.

Google Tag Manager (Google LLC)

Google Tag Manager is a tag management service provided by Google LLC.

Personal Data processed: Tracker; Usage Data.

Place of processing: United States – Privacy Policy.

Category of personal information collected according to CCPA: internet information.

This processing constitutes a sale based on the denition under the CCPA. In addition to the information in this clause, the User can nd information regarding how to opt out of the sale in the section detailing the rights of Californian consumers.

User database management

This type of service allows the Owner to build user proles by starting from an email address, a personal name, or other information that the User provides to this Website, as well as to track User activities through analytics features. This Personal Data may also be matched with publicly available information about the User (such as social networks' proles) and used to build private proles that the Owner can display and use for improving this Website.

Some of these services may also enable the sending of timed messages to the User, such as emails based on specic actions performed on this Website.

ZOHO CRM (Zoho Corporation Pvt. Ltd.)

ZOHO CRM is a User database management service provided by Zoho Corporation Pvt. Ltd.

Personal Data processed: address; email address; rst name; last name; phone number; various types of Data as specified in the privacy policy of the service.

Place of processing: United States – Privacy Policy.

Category of personal information collected according to CCPA: identifiers; internet information.

This processing constitutes a sale based on the definition under the CCPA. In addition to the information in this clause, the User can find information regarding how to opt out of the sale in the section detailing the rights of Californian consumers.

The rights of Users

Users may exercise certain rights regarding their Data processed by the Owner.

In particular, Users have the right to do the following:

- **Withdraw their consent at any time.** Users have the right to withdraw consent where they have previously given their consent to the processing of their Personal Data.
- **Object to processing of their Data.** Users have the right to object to the processing of their Data if the processing is carried out on a legal basis other than consent. Further details are provided in the dedicated section below.

- **Access their Data.** Users have the right to learn if Data is being processed by the Owner, obtain disclosure regarding certain aspects of the processing and obtain a copy of the Data undergoing processing.

- **Verify and seek rectification.** Users have the right to verify the accuracy of their Data and ask for it to be updated or corrected.

- **Restrict the processing of their Data.** Users have the right, under certain circumstances, to restrict the processing of their Data. In this case, the Owner will not process their Data for any purpose other than storing it.

- **Have their Personal Data deleted or otherwise removed.** Users have the right, under certain circumstances, to obtain the erasure of their Data from the Owner.

- **Receive their Data and have it transferred to another controller.** Users have the right to receive their Data in a structured, commonly used and machine readable format and, if technically feasible, to have it transmitted to another controller without any hindrance. This provision is applicable provided that the Data is processed by automated means and that the processing is based on the User's consent, on a contract which the User is part of or on pre-contractual obligations thereof.

- **Lodge a complaint.** Users have the right to bring a claim before their competent data protection authority.

Details about the right to object to processing

Where Personal Data is processed for a public interest, in the exercise of an official authority vested in the Owner or for the purposes of the legitimate interests pursued by the Owner, Users may object to such processing by providing a ground related to their particular situation to justify the objection.

Users must know that, however, should their Personal Data be processed for direct marketing purposes, they can object to that processing at any time without providing any justification. To learn, whether the Owner is processing Personal Data for direct marketing purposes, Users may refer to the relevant sections of this document.

How to exercise these rights
Any requests to exercise User rights can be directed to the Owner through the contact details provided in this document. These requests can be exercised free of charge and will be addressed by the Owner as early as possible and always within one month.

Cookie Policy
This Website uses Trackers. To learn more, the User may consult the Cookie Policy.<

Additional information about Data collection and processing

Legal action
The User's Personal Data may be used for legal purposes by the Owner in Court or in the stages leading to possible legal action arising from improper use of this Website or the related Services.
The User declares to be aware that the Owner may be required to reveal personal data upon request of public authorities.

Additional information about User's Personal Data
In addition to the information contained in this privacy policy, this Website may provide the User with additional and contextual information concerning particular Services or the collection and processing of Personal Data upon request.

System logs and maintenance
For operation and maintenance purposes, this Website and any third-party services may collect les that record interaction with this Website (System logs) use other Personal Data (such as the IP Address) for this purpose.

Information not contained in this policy
More details concerning the collection or processing of Personal Data may be requested from the Owner at any time. Please see the contact information at the beginning of this document.

How "Do Not Track" requests are handled
This Website does not support "Do Not Track" requests.
To determine whether any of the third-party services it uses honor the "Do Not Track" requests, please read their privacy policies.

Changes to this privacy policy
The Owner reserves the right to make changes to this privacy policy at any time by notifying its Users on this page and possibly within this Website and/or – as far as technically and legally feasible – sending a notice to Users via any contact information

available to the Owner. It is strongly recommended to check this page often, referring to the date of the last modification listed at the bottom.

Should the changes affect processing activities performed on the basis of the User's consent, the Owner shall collect new consent from the User, where required.

<h3″>Information for Californian consumers </h3″>

This part of the document integrates with and supplements the information contained in the rest of the privacy policy and is provided by the business running this Website and, if the case may be, its parent, subsidiaries and aliates (for the purposes of this section referred to collectively as "we", "us", "our").

The provisions contained in this section apply to all Users who are consumers residing in the state of California, United States of America, according to "The California Consumer Privacy Act of 2018" (Users are referred to below, simply as "you", "your", "yours"), and, for such consumers, these provisions supersede any other possibly divergent or conflicting provisions contained in the privacy policy.

This part of the document uses the term "personal information" as it is defined in The California Consumer Privacy Act (CCPA).

Categories of personal information collected, disclosed or sold

In this section we summarize the categories of personal information that we've collected, disclosed or sold and the purposes thereof. **You can read about these activities in detail in the section titled "Detailed information on the processing of Personal Data" within this document.**

Information we collect: the categories of personal information we collect

We have collected the following categories of personal information about you: identifiers, commercial information and internet information.

We will not collect additional categories of personal information without notifying you.

How we collect information: what are the sources of the personal information we collect?

We collect the above mentioned categories of personal information, either directly or indirectly, from you when you use this Website.

For example, you directly provide your personal information when you submit requests via any forms on this Website. You also provide personal information indirectly when you navigate this Website, as personal information about you is automatically observed and collected. Finally, we may collect your personal information from third parties that work with us in connection with the Service or with the functioning of this Website and features thereof.

How we use the information we collect: sharing and disclosing of your personal information with third parties for a business purpose

We may disclose the personal information we collect about you to a third party for business purposes. In this case, we enter a written agreement with such third party that requires the recipient to both keep the personal information confidential and not use it for any purpose(s) other than those necessary for the performance of the agreement.

We may also disclose your personal information to third parties when you explicitly ask or authorize us to do so, in order to provide you with our Service.

To find out more about the purposes of processing, please refer to the relevant section of this document.

Sale of your personal information

For our purposes, the word “sale” means any “selling, renting, releasing, disclosing, disseminating, making available, transferring or otherwise communicating orally, in writing, or by electronic means, a consumer’s personal information by the business to **another business or a third party, for monetary or other valuable consideration”.**

This means that, for example, a sale can happen whenever an application runs ads, or makes statistical analyses on the trac or views, or simply because it uses tools such as social network plugins and the like.

Your right to opt out of the sale of personal information
You have the right to opt out of the sale of your personal information. This means that whenever you request us to stop selling your data, we will abide by your request.
Such requests can be made freely, at any time, without submitting any verifiable request, simply by following the instructions below.

Instructions to opt out of the sale of personal information
If you’d like to know more, or exercise your right to opt out in regard to all the sales carried out by this Website, both online and offline, you can contact us for further information using the contact details provided in this document.

What are the purposes for which we use your personal information?
We may use your personal information to allow the operational functioning of this Website and features thereof (“business purposes”). In such cases, your personal information will be processed in a fashion necessary and proportionate to the business purpose for which it was collected, and strictly within the limits of compatible operational purposes.

We may also use your personal information for other reasons such as for commercial purposes (as indicated within the section “Detailed information on the processing of Personal Data” within this document), as well as for complying with the law and defending our

rights before the competent authorities where our rights and interests are threatened or we suer an actual damage.

We will not use your personal information for different, unrelated, or incompatible purposes without notifying you.

Your California privacy rights and how to exercise them

The right to know and to portability
You have the right to request that we disclose to you:

- the categories and sources of the personal information that we collect about you, the purposes for which we use your information and with whom such information is shared;
- in case of sale of personal information or disclosure for a business purpose, two separate lists where we disclose:
    - for sales, the personal information categories purchased by each category of recipient; and
    - for disclosures for a business purpose, the personal information categories obtained by each category of recipient.

The disclosure described above will be limited to the personal information collected or used over the past 12 months.

If we deliver our response electronically, the information enclosed will be “portable”, i.e. delivered in an easily usable format to enable you to transmit the information to another entity without hindrance – provided that this is technically feasible.

The right to request the deletion of your personal information

You have the right to request that we delete any of your personal information, subject to exceptions set forth by the law (such as, including but not limited to, where the information is used to identify and repair errors on this Website, to detect security incidents and protect against fraudulent or illegal activities, to exercise certain rights etc.).

If no legal exception applies, as a result of exercising your right, we will delete your personal information and direct any of our service providers to do so.

How to exercise your rights
To exercise the rights described above, you need to submit your verifiable request to us by contacting us via the details provided in this document.

For us to respond to your request, it’s necessary that we know who you are. Therefore, you can only exercise the above rights by making a verifiable request which must:

- provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative;
- describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We will not respond to any request if we are unable to verify your identity and therefore confirm the personal information in our possession actually relates to you.

If you cannot personally submit a verifiable request, you can authorize a person registered with the California Secretary of State to act on your behalf.

If you are an adult, you can make a verifiable request on behalf of a minor under your parental authority.

You can submit a maximum number of 2 requests over a period of 12 months.

How and when we are expected to handle your request

We will confirm receipt of your verifiable request within 10 days and provide information about how we will process your request.

We will respond to your request within 45 days of its receipt. Should we need more time, we will explain to you the reasons why, and how much more time we need. In this regard, please note that we may take up to 90 days to fulfill your request.

Our disclosure(s) will cover the preceding 12 month period.

Should we deny your request, we will explain you the reasons behind our denial.

We do not charge a fee to process or respond to your verifiable request unless such request is manifestly unfounded or excessive. In such cases, we may charge a reasonable fee, or refuse to act on the request. In either case, we will communicate our choices and explain the reasons behind it.

Definitions and legal references

Personal Data (or Data)
Any information that directly, indirectly, or in connection with other information — including a personal identification number — allows for the identification or identifiability of a natural person.

Usage Data

Information collected automatically through this Website (or third-party services employed in this Website), which can include: the IP addresses or domain names of the computers utilized by the Users who use this Website, the URI addresses (Uniform Resource Identifier), the time of the request, the method utilized to submit the request to the server, the size of the le received in response, the numerical code indicating the status of the server's answer (successful outcome, error, etc.), the country of origin, the features of the browser and the operating system utilized by the User, the various time details per visit (e.g., the time spent on each page within the Application) and the details about the path followed within the Application with special reference to the sequence of pages visited, and other parameters about the device operating system and/or the User's IT environment.

User
The individual using this Website who, unless otherwise specified, coincides with the Data Subject.

Data Subject

The natural person to whom the Personal Data refers.

Data Processor (or Data Supervisor)
The natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller, as described in this privacy policy.

Data Controller (or Owner)
The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data, including the security measures concerning the operation and use of this Website. The Data Controller, unless otherwise specified, is the Owner of this Website.

This Website (or this Application)
The means by which the Personal Data of the User is collected and processed.

Service
The service provided by this Website as described in the relative terms (if available) and on this site/application.

European Union (or EU)
Unless otherwise specified, all references made within this document to the European Union include all current member states to the European Union and the European Economic Area.

Cookie

Cookies are Trackers consisting of small sets of data stored in the User's browser.

Tracker
Tracker indicates any technology – e.g Cookies, unique identifiers, web beacons, embedded scripts, e-tags and fingerprinting – that enables the tracking of Users, for example by accessing or storing information on the User's device.

Legal information

This privacy statement has been prepared based on provisions of multiple legislations, including Art. 13/14 of Regulation (EU) 2016/679 (General Data Protection Regulation).

This privacy policy relates solely to this Website, if not stated otherwise within this document.

Latest update: August 30, 2021

Terms of Service | Our Privacy Policy | FAQ
P.O. Box 513018, Los Angeles, CA 90051